09/936685
FR00/00680

REPUBLIQUE FRANÇAISE

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

REC'D 26 APR 2000
WIPO PCT

EV

BREVET D'INVENTION

CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION

COPIE OFFICIELLE

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

Fait à Paris, le 12 AVR. 2000

Pour le Directeur général de l'Institut
national de la propriété industrielle
Le Chef du Département des brevets

Martine PLANCHE

DOCUMENT DE PRIORITÉ

PRÉSENTÉ OU TRANSMIS CONFORMÉMENT À LA REGLE 17.1.a) OU b)

CERTIFIED COPY OF PRIORITY DOCUMENT

INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE
SIEGE
26 bis, rue de Saint Petersbourg
75800 PARIS Cédex 08
Téléphone : 01 53 04 53 04
Télécopie : 01 42 93 59 30

ETABLISSEMENT PUBLIC NATIONAL CREE PAR LA LOI N° 51-444 DU 19 AVRIL 1951

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : 01 53 04 53 04 Télécopie : 01 42 93 59 30

BREVET D'INVENTION, CERTIFICAT D'UTILITE

Code de la propriété intellectuelle-Livre VI

cerfa N° 55 -1328

REQUÊTE EN DÉLIVRANCE

Confirmation d'un dépôt par télécopie ☐

Cet imprimé est à remplir à l'encre noire en lettres capitales

Réservé à l'INPI

DATE DE REMISE DES PIÈCES 17 0399

N° D'ENREGISTREMENT NATIONAL 99 03329

DÉPARTEMENT DE DÉPÔT 75

DATE DE DÉPÔT 17 MARS 1999

1 NOM ET ADRESSE DU DEMANDEUR OU DU MANDATAIRE À QUI LA CORRESPONDANCE DOIT ÊTRE ADRESSÉE

SCHLUMBERGER SYSTEMES
Test & Transactions
50 Av. Jean Jaurès - B.P 620-04
92542 MONTROUGE Cédex
A l'attention de Anne DANG TRAN

n°du pouvoir permanent / références du correspondant / téléphone
PG07391 76-0543 01 47 46 72 14

2 DEMANDE Nature du titre de propriété industrielle

☒ brevet d'invention ☐ demande divisionnaire ☐ certificat d'utilité ☐ transformation d'une demande de brevet européen

demande initiale : ☐ brevet d'invention ☐ certificat d'utilité n° date

Établissement du rapport de recherche ☐ différé ☒ immédiat

Le demandeur, personne physique, requiert le paiement échelonné de la redevance ☐ oui ☒ non

Titre de l'invention (200 caractères maximum)

PROCEDE DE CHARGEMENT SECURISE DE DONNEES ENTRE DES MODULES DE SECURITE

3 DEMANDEUR (S) n° SIREN 5 6 2 1 1 3 5 3 0 code APE-NAF

Nom et prénoms (souligner le nom patronymique) ou dénomination

SCHLUMBERGER SYSTEMES

Forme juridique

Société Anonyme

Nationalité (s)

Française

Adresse (s) complète (s)

50, avenue Jean Jaurès
92120 MONTROUGE

Pays

France

En cas d'insuffisance de place, poursuivre sur papier libre ☐

4 INVENTEUR (S) Les inventeurs sont les demandeurs ☐ oui ☒ non Si la réponse est non, fournir une désignation séparée

5 RÉDUCTION DU TAUX DES REDEVANCES ☐ requise pour la 1ère fois ☐ requise antérieurement au dépôt ; joindre copie de la décision d'admission

6 DÉCLARATION DE PRIORITÉ OU REQUÊTE DU BÉNÉFICE DE LA DATE DE DÉPÔT D'UNE DEMANDE ANTÉRIEURE

pays d'origine	numéro	date de dépôt	nature de la demande
SANS			

7 DIVISIONS antérieures à la présente demande n° date n° date

8 SIGNATURE DU DEMANDEUR OU DU MANDATAIRE
(nom et qualité du signataire - n° d'inscription)

Anne DANG TRAN
Mandataire
(PG07391)

SIGNATURE DU PRÉPOSÉ À LA RÉCEPTION SIGNATURE APRÈS ENREGISTREMENT DE LA DEMANDE À L'INPI

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

BREVET D'INVENTION, CERTIFICAT D'UTILITE

DÉSIGNATION DE L'INVENTEUR
(si le demandeur n'est pas l'inventeur ou l'unique inventeur)

DEPARTEMENT DES BREVETS

26bis, rue de Saint-Pétersbourg
75800 Paris Cédex 08
Tél. : 01 53 04 53 04 - Télécopie : 01 42 93 59 30

76-0543

N° D'ENREGISTREMENT NATIONAL

9903329

TITRE DE L'INVENTION :

PROCEDE DE CHARGEMENT SECURISE DE DONNEES ENTRE DES MODULES DE SECURITE

LE(S) SOUSSIGNÉ(S)

Anne DANG TRAN
SCHLUMBERGER SYSTEMES
Test & Transactions
50, avenue Jean Jaurès - BP 620-04
92542 MONTROUGE Cédex

DÉSIGNE(NT) EN TANT QU'INVENTEUR(S) (indiquer nom, prénoms, adresse et souligner le nom patronymique) :

DOLLET Richard
15 rue Poirier de Narçay
75014 PARIS
FRANCE

NOTA : A titre exceptionnel, le nom de l'inventeur peut être suivi de celui de la société à laquelle il appartient (société d'appartenance) lorsque celle-ci est différente de la société déposante ou titulaire.

Date et signature (s) du (des) demandeur (s) ou du mandataire

Le 16 mars 1999

Anne DANG TRAN
(PG 07391)

BA 113/140897

PROCEDE DE CHARGEMENT SECURISE DE DONNEES ENTRE DES MODULES DE SECURITE

La présente invention concerne un procédé de chargement sécurisé de données secrètes à partir d'un premier module de sécurité vers au moins un deuxième module de sécurité, ledit premier module comportant au moins un fichier de données secrètes, ledit deuxième module comportant une première mémoire non volatile et une deuxième mémoire volatile.

L'invention trouve une application particulièrement avantageuse dans le domaine de la téléphonie.

Dans le domaine de la téléphonie, il existe des systèmes d'administration de terminaux qui comportent un premier module de sécurité embarqué dans un serveur d'administration et des deuxièmes modules de sécurité généralement embarqués dans les terminaux précités. Les terminaux sont appelés publiphones.

Un deuxième module de sécurité garantit la validité d'une carte utilisateur introduite dans un publiphone, notamment grâce à une authentification de ladite carte. A cet effet, ledit deuxième module de sécurité comprend dans sa première mémoire des données secrètes permettant de garantir ladite validité des cartes utilisateurs. Les systèmes d'administration de publiphones ainsi que les données secrètes sont gérés par des opérateurs de téléphonie. Afin de diminuer les risques de fraude consistant à espionner un réseau de communication reliant le serveur et les publiphones et ainsi à découvrir lesdites données secrètes, les opérateurs sont amenés à modifier régulièrement tout ou partie des données secrètes d'un deuxième module de sécurité d'un publiphone, à partir de données secrètes contenues dans un fichier du premier module de sécurité.

Un procédé connu de la technique comprend les étapes selon lesquelles :

- on chiffre les données secrètes du premier module de sécurité qui doivent être transmises au deuxième module de sécurité et qui se trouvent dans le serveur d'administration,
- le publiphone se connecte au serveur d'administration lorsqu'aucune conversation n'est en cours,
- les données secrètes sont transmises au deuxième module de sécurité se trouvant dans le publiphone.

Lorsque le publiphone se connecte au serveur d'administration, il est indisponible à tout utilisateur, ainsi la connexion se fait généralement la nuit. L'échange de données se fait en mode déconnecté appelé dans le langage anglo-saxon mode "off-line".

Afin de diversifier les transmissions de données secrètes, on fait intervenir une donnée pseudo-aléatoire basée sur une valeur d'un compteur contenu dans le deuxième module de sécurité. A chaque échange de données secrètes, la valeur du compteur est incrémentée, le premier module de sécurité doit connaître la valeur dudit compteur et incrémenter un compteur local dédié audit deuxième module.

Bien que ce procédé permette un chargement de données secrètes entre un premier et deuxième modules de sécurité, il nécessite une administration lourde de bases de données permettant de garantir la synchronisation des différents compteurs. En effet, une trace de l'ensemble des échanges effectués avec un deuxième module de sécurité doit être conservée. De plus, ce procédé ne garantit pas un échange de données parfaitement diversifié.

Aussi, un problème technique à résoudre par l'objet de la présente invention est de proposer un procédé de chargement sécurisé de données secrètes à partir d'un premier module de sécurité vers au moins un deuxième module de sécurité, ledit premier module comportant au moins un fichier de données secrètes, ledit deuxième module comportant une première mémoire non volatile et une deuxième

mémoire volatile, qui permettrait de garantir un échange de données parfaitement diversifié entre un premier et deuxième modules de sécurité, en mode "off-line", tout en évitant une gestion trop lourde de bases de données.

Une solution au problème technique posé se caractérise, selon l'invention, en ce que ledit procédé de chargement comporte les étapes selon lesquelles :

- on génère au moins une donnée aléatoire dans la deuxième mémoire du deuxième module,
- on enregistre des informations comprenant ladite donnée aléatoire dans la première mémoire du deuxième module,
- on envoie au premier module la donnée aléatoire,
- dans le premier module, on chiffre une donnée secrète du fichier dudit premier module, à partir de la donnée aléatoire et d'un algorithme de cryptage,
- on envoie au deuxième module ladite donnée secrète chiffrée,
- on transfère les informations, comprenant la donnée aléatoire de la première mémoire du deuxième module, de ladite première mémoire vers la deuxième mémoire dudit module,
- on déchiffre ladite donnée secrète chiffrée, à partir d'un algorithme de décryptage et de la donnée aléatoire, et, on enregistre dans le deuxième module, ladite donnée secrète déchiffrée.

Ainsi, comme on le verra en détail plus loin, le procédé de chargement de l'invention permet, en utilisant une donnée aléatoire pour le chargement des données secrètes, d'améliorer la sécurité du chargement des données en diversifiant de façon parfaite les données transmises. Ainsi, un fraudeur qui espionne un réseau de communication et récupère les données transmises n'obtient jamais une même valeur de chiffrement et ne peut par conséquent découvrir

un secret relatif aux données secrètes transmises. De plus, le fait d'enregistrer la donnée aléatoire dans une mémoire non volatile du deuxième module de sécurité permet de l'utiliser en mode "off-line", puisque ladite donnée aléatoire n'est pas perdue lorsque ledit deuxième module de sécurité est mis hors tension.

La description qui va suivre au regard des dessins annexés, donnée à titre d'exemple non limitatif, fera bien comprendre en quoi consiste l'invention et comment elle peut être réalisée.

La figure 1 est un schéma montrant un premier module de sécurité et plusieurs deuxièmes modules de sécurité.

La figure 2 est un schéma montrant le premier module et un deuxième module de la figure 1.

La figure 3 est un schéma montrant un échange de données entre le premier module et le deuxième module de la figure 2.

La figure 4 un schéma montrant un deuxième échange de données entre le premier module et le deuxième module de la figure 2.

La figure 5 un schéma montrant un troisième échange de données entre le premier module et le deuxième module de la figure 2.

Sur la figure 1 est représenté un premier module S de sécurité et plusieurs deuxièmes modules SAM de sécurité, chaque deuxième module SAM comprenant une première mémoire M1 non volatile et une deuxième mémoire M2 volatile appelée mémoire de travail. La figure 2 montre le premier module S et un deuxième module SAM. Le premier module S comporte au moins un fichier EF1 de données secrètes DATA et un algorithme ALGO de cryptage. Un fichier de données secrètes est généralement associé à un opérateur de téléphonie donné. Le deuxième module SAM comporte un algorithme ALGOP de décryptage inverse de l'algorithme ALGO de cryptage et des données secrètes DATA.

Afin de modifier une donnée secrète du deuxième module SAM, il faut charger une donnée secrète à partir du fichier EF1 du premier

module S de sécurité. Le chargement doit se faire de façon sécurisée. La donnée secrète est ainsi transmise de manière chiffrée. La phase de chargement comprend plusieurs étapes décrites ci-après.

Dans une première étape, on génère au moins une donnée aléatoire RAND dans la mémoire M2 volatile du deuxième module SAM.

Dans une deuxième étape, comme le montre la figure 3, on enregistre des informations INFO comprenant ladite donnée aléatoire RAND dans la mémoire M1 non volatile du deuxième module SAM. Un emplacement mémoire dans ladite mémoire M1 non volatile est réservé à cet effet et est initialisé par défaut à une valeur d'initialisation V.

Dans un premier mode de réalisation, les informations INFO, comprenant ladite donnée aléatoire RAND, comportent un indice relatif à une donnée secrète DATA. L'indice étant par exemple un numéro de donnée secrète à modifier ou un indice d'emplacement mémoire dans lequel une donnée secrète doit être chargée dans le deuxième module SAM. Ainsi, dans le cas où le deuxième module SAM est mis hors tension pour des raisons d'économie d'énergie, la donnée aléatoire RAND et les informations associées ne sont pas perdues.

Dans une troisième étape, on envoie au premier module S la donnée aléatoire RAND. On notera que la deuxième et la troisième étape peuvent être permutées.

Afin de réduire le nombre d'accès au deuxième module SAM, la génération et l'envoi de la donnée aléatoire RAND ainsi que l'enregistrement des informations INFO dans le deuxième module SAM, se font au moyen d'une première commande ASKLOADING. Cette première commande est envoyée par le serveur d'administration au deuxième module SAM via le publiphone (non représenté).

Dans une quatrième étape, dans le premier module S, on chiffre la donnée secrète DATA du fichier EF1 qui doit être transmise dans le deuxième module SAM. Le chiffrement comprend une étape de cryptage

utilisant l'algorithme ALGO de cryptage et la donnée aléatoire RAND. L'utilisation de la donnée aléatoire RAND évite d'avoir une même valeur de chiffrement pour une donnée secrète DATA. Ainsi, un fraudeur pourra difficilement faire un lien entre les différentes données transmises sur le réseau de communication, celles-ci étant différentes à chaque transmission. Le chiffrement peut également comprendre, d'une part, une étape de signature de la donnée secrète DATA basée sur la donnée aléatoire RAND, et, d'autre part, une étape de certification des données transmises. La signature permet de vérifier l'authenticité de la donnée secrète DATA chargée et le certificat permet de vérifier l'intégrité des données transmises.

Dans une cinquième étape, comme le montre la figure 4, on envoie au deuxième module SAM ladite donnée secrète chiffrée DATAC.

Dans une sixième étape, on transfère les informations INFO, comprenant la donnée aléatoire RAND de la mémoire M1 non volatile du deuxième module SAM, de ladite mémoire M1 vers la mémoire M2 de travail dudit module SAM. Ainsi, on récupère dans la mémoire M2 de travail, la donnée aléatoire RAND, qui a été utilisée pour chiffrer la donnée secrète DATA, ainsi que les informations associées.

La duplication de la donnée aléatoire RAND et des informations associées dans deux mémoires différentes du deuxième module SAM peut générer des incohérences dans ledit module et des problèmes de sécurité. Aussi, on ne garde qu'un seul jeu d'informations INFO dans le deuxième module SAM. A cet effet, postérieurement à l'enregistrement des informations INFO comprenant ladite donnée aléatoire RAND dans la première mémoire M1 du deuxième module SAM (figure 3), on efface les informations INFO se trouvant dans la deuxième mémoire M2 dudit deuxième module SAM. De la même manière, postérieurement au transfert des informations INFO comprenant la donnée aléatoire RAND, de la première mémoire M1 du deuxième module SAM dans la deuxième

mémoire M2 dudit module (figure 4), on efface lesdites informations INFO dans ladite première mémoire M1.

Enfin, dans une dernière étape, on déchiffre ladite donnée secrète chiffrée DATAC, à partir de l'algorithme ALGOP de décryptage du deuxième module SAM et de la donnée aléatoire RAND, et, on enregistre dans le deuxième module SAM ladite donnée secrète DATA déchiffrée.

Afin de réduire le nombre d'accès au deuxième module SAM, le transfert des informations INFO, le déchiffrement de la donnée secrète DATA dans le deuxième module SAM et l'enregistrement, se font au moyen d'une deuxième commande ADMINRECOVER. Cette deuxième commande est envoyée par le serveur d'administration au deuxième module SAM via le publiphone (non représenté). Dans le cas où un incident survient lors du chargement, ou à la fin dudit chargement, l'emplacement mémoire, dans la mémoire M1 non volatile, où se trouvent les informations INFO comprenant la donnée aléatoire RAND, est réinitialisé à la valeur d'initialisation V . Si un incident est survenu, une autre donnée aléatoire RAND est générée et les différentes étapes du procédé décrites ci-dessus sont effectuées de nouveau. Lorsque la deuxième commande ADMINRECOVER est envoyée, on vérifie qu'une donnée aléatoire RAND a été générée et enregistrée. Ainsi, on vérifie que l'emplacement mémoire de la première mémoire M1 non volatile du deuxième module SAM, réservé à la donnée aléatoire RAND, ne comporte pas la valeur d'initialisation V. Si tel est le cas, la deuxième commande ADMINRECOVER est exécutée. Dans le cas contraire, elle n'est pas exécutée et on effectue la première étape du procédé.

Généralement, un deuxième module SAM gère différents types de carte utilisateur et comporte par suite plusieurs données secrètes DATA associées à chaque type de carte utilisateur, un type de carte correspondant communément à un opérateur donné, fournisseur desdites cartes. Il est habituel de vouloir modifier l'ensemble des

données secrètes DATA associées à un type de cartes. Dans ce cas, on effectue les premières étapes du procédé de l'invention comme décrit précédemment, mais en les appliquant à l'ensemble des données secrètes DATA à modifier. Ainsi, on génère successivement plusieurs données aléatoires RAND dans la deuxième mémoire M2 du deuxième module SAM et on enregistre dans la première mémoire M1 du deuxième module SAM, consécutivement à chaque génération de donnée aléatoire RAND, les informations INFO comprenant la donnée aléatoire RAND générée. Comme le montre l'exemple de la figure 5, on génère trois données aléatoires RAND1, RAND2 et RAND3 dans le deuxième module SAM et on les enregistre dans la mémoire M1 non volatile dudit module. Par la suite, on envoie les trois données aléatoires générées au premier module S du serveur d'administration. On chiffre trois données secrètes DATA1, DATA2 et DATA3 se trouvant dans le fichier EF1 du premier module S et correspondant aux trois données secrètes à modifier dans le deuxième module SAM. La correspondance est effectuée grâce par exemple à trois indices (1,2 et 3) de donnée secrète envoyés en même temps que les trois données aléatoires RAND. Enfin, pour transmettre les trois données secrètes DATA1, DATA2 et DATA3 dans ledit deuxième module SAM, on effectue toutes les étapes du procédé de l'invention comme décrit précédemment, à partir de la cinquième étape pour chaque donnée secrète DATA à charger ou pour l'ensemble des données secrètes DATA comme avec les précédentes étapes.

Ainsi, suivant un premier mode de réalisation du chargement de plusieurs données décrit ci-dessus, lors de chaque chargement, on utilise une donnée aléatoire RAND pour charger une donnée secrète DATA. Suivant un second mode de réalisation, afin de diminuer le temps de chargement des données secrètes, lors de chaque chargement,

on utilise une unique donnée aléatoire RAND pour charger plusieurs données secrètes DATA.

Bien entendu, l'invention n'est nullement limitée au domaine de la téléphonie, elle peut s'étendre à d'autres domaines dans lesquels est mis en oeuvre un système d'échange de données entre un module centralisé disposant de données secrètes et des modules délocalisés aptes à recevoir lesdites données secrètes.

REVENDICATIONS

1 - Procédé de chargement sécurisé de données secrètes à partir d'un premier module (S) de sécurité vers au moins un deuxième module (SAM) de sécurité, ledit premier module (S) comportant au moins un fichier (EF1) de données secrètes (DATA), ledit deuxième module (SAM) comportant une première mémoire (M1) non volatile et une deuxième mémoire (M2) volatile, caractérisé en ce qu'il comporte les étapes selon lesquelles :

- on génère au moins une donnée aléatoire (RAND) dans la deuxième mémoire (M2) du deuxième module (SAM),
- on enregistre des informations (INFO) comprenant ladite donnée aléatoire (RAND) dans la première mémoire (M1) du deuxième module (SAM),
- on envoie au premier module (S) la donnée aléatoire (RAND),
- dans le premier module (S), on chiffre une donnée secrète (DATA) du fichier (EF1) dudit premier module (S), à partir de la donnée aléatoire (RAND) et d'un algorithme (ALGO) de cryptage,
- on envoie au deuxième module (SAM) ladite donnée secrète chiffrée (DATAC),
- on transfère les informations (INFO), comprenant la donnée aléatoire (RAND) de la première mémoire (M1) du deuxième module (SAM), de ladite première mémoire (M1) vers la deuxième mémoire (M2) dudit module (SAM),
- on déchiffre ladite donnée secrète chiffrée (DATAC), à partir d'un algorithme (ALGOP) de décryptage et de la donnée aléatoire (RAND), et, on enregistre dans le deuxième module (SAM), ladite donnée secrète (DATA) déchiffrée.

2 - Procédé selon l'une des revendications précédentes, caractérisé en ce qu'il comporte une étape supplémentaire selon laquelle :

- postérieurement à l'enregistrement des informations (INFO) comprenant ladite donnée aléatoire (RAND) dans la première mémoire (M1) du deuxième module (SAM), on efface les informations (INFO) se trouvant dans la deuxième mémoire (M2) dudit deuxième module (SAM).

3 - Procédé selon l'une des revendications précédentes, caractérisé en ce qu'il comporte une étape supplémentaire selon laquelle :

- postérieurement au transfert des informations (INFO) comprenant la donnée aléatoire (RAND), de la première mémoire (M1) du deuxième module (SAM) dans la deuxième mémoire (M2) dudit module, on efface lesdites informations (INFO) dans ladite première mémoire (M1).

4 - Procédé selon l'une des revendications précédentes, caractérisé en ce que la génération et l'envoi de la donnée aléatoire (RAND) ainsi que l'enregistrement des informations (INFO) dans le deuxième module (SAM), se font au moyen d'une première commande (ASKLOADING).

5 - Procédé selon l'une des revendications précédentes, caractérisé en ce que le transfert des informations (INFO), le déchiffrement de la donnée secrète (DATA) dans le deuxième module (SAM) et l'enregistrement, se font au moyen d'une deuxième commande (ADMINRECOVER).

6 - Procédé selon l'une des revendications précédentes, caractérisé en ce que les informations (INFO), comprenant ladite donnée aléatoire (RAND), comportent un indice relatif à une donnée secrète (DATA).

7 - Procédé selon l'une des revendications précédentes, caractérisé en ce que l'on génère successivement plusieurs données aléatoires (RAND) dans la deuxième mémoire (M2) du deuxième module (SAM) et on enregistre dans la première mémoire (M1) du deuxième module (SAM), consécutivement à chaque génération de donnée aléatoire (RAND), les informations (INFO) comprenant la donnée aléatoire (RAND) générée.

8 - Procédé selon l'une des revendications précédentes, caractérisé en ce que, lors de chaque chargement, on utilise une donnée aléatoire RAND pour charger une donnée secrète DATA.

9 - Procédé selon l'une des revendications 1 à 7, caractérisé en ce que, lors de chaque chargement, on utilise une unique donnée aléatoire RAND pour charger plusieurs données secrètes DATA.

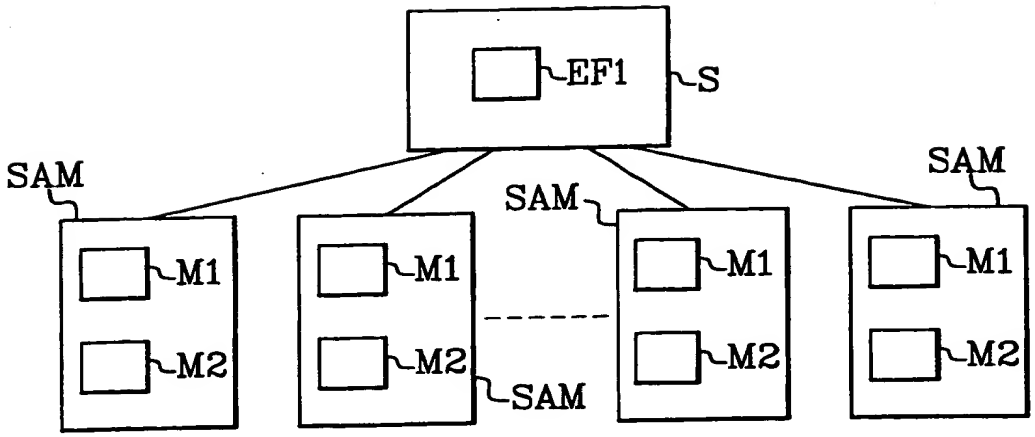

FIG.1

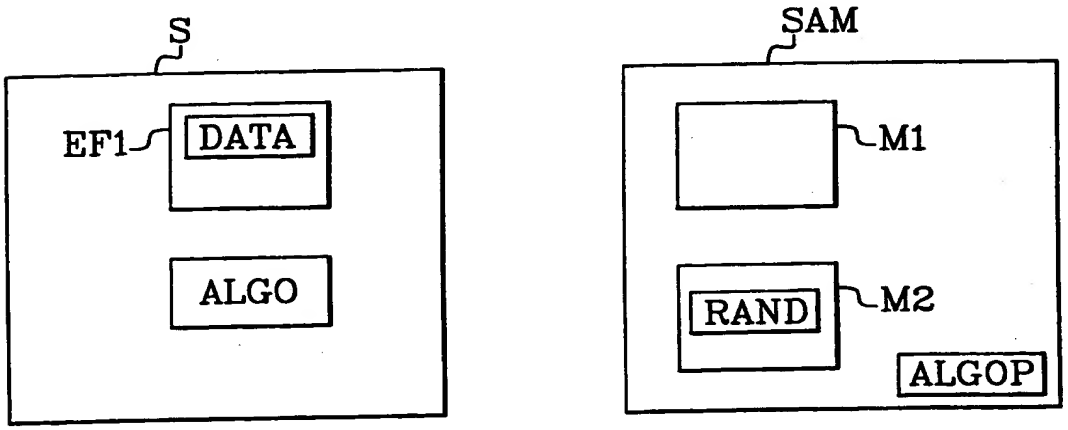

FIG.2

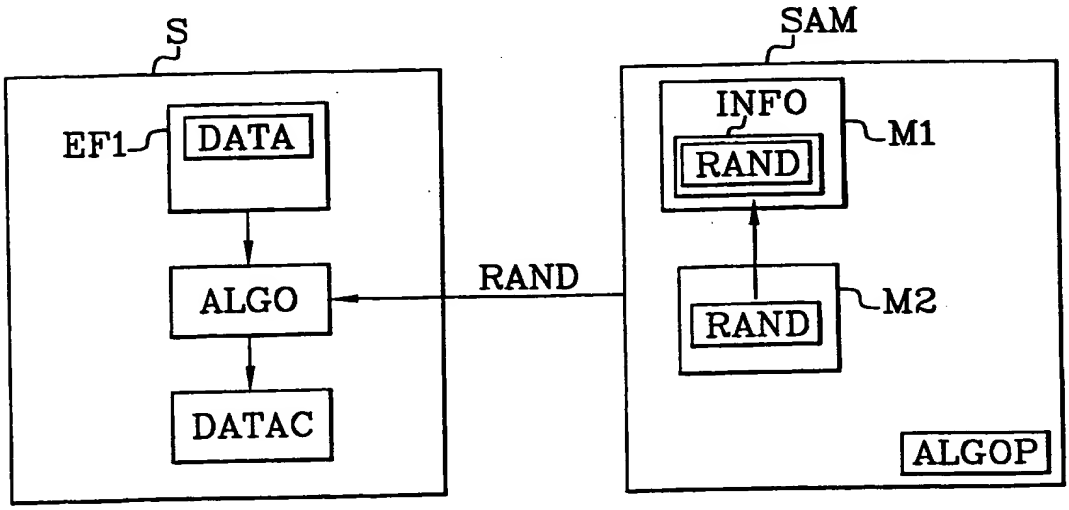

FIG.3

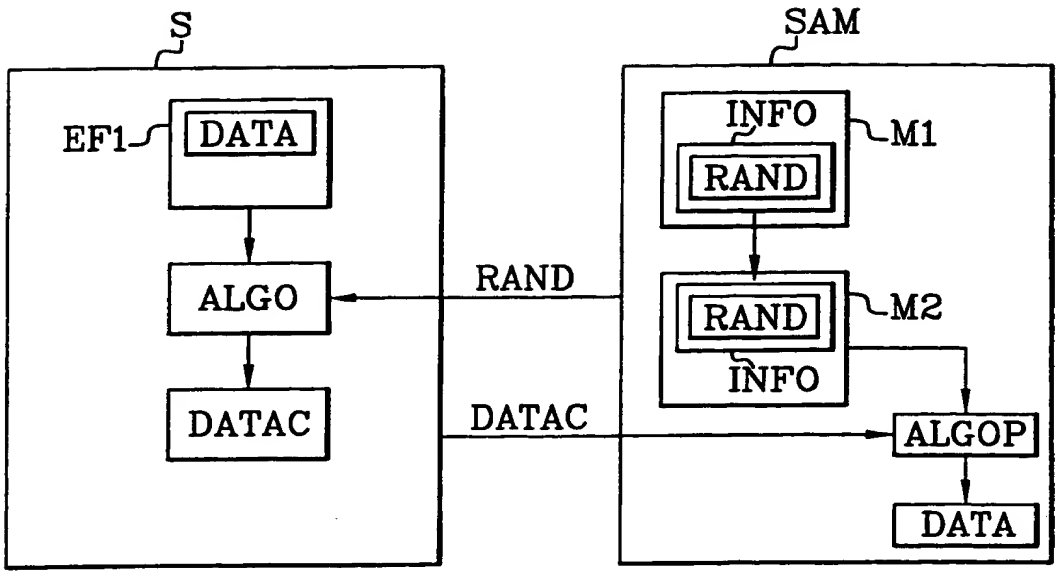
S
SAM
EF1
DATA
ALGO
DATAC
RAND
INFO
M1
RAND
RAND
M2
INFO
DATAC
ALGOP
DATA

FIG.4

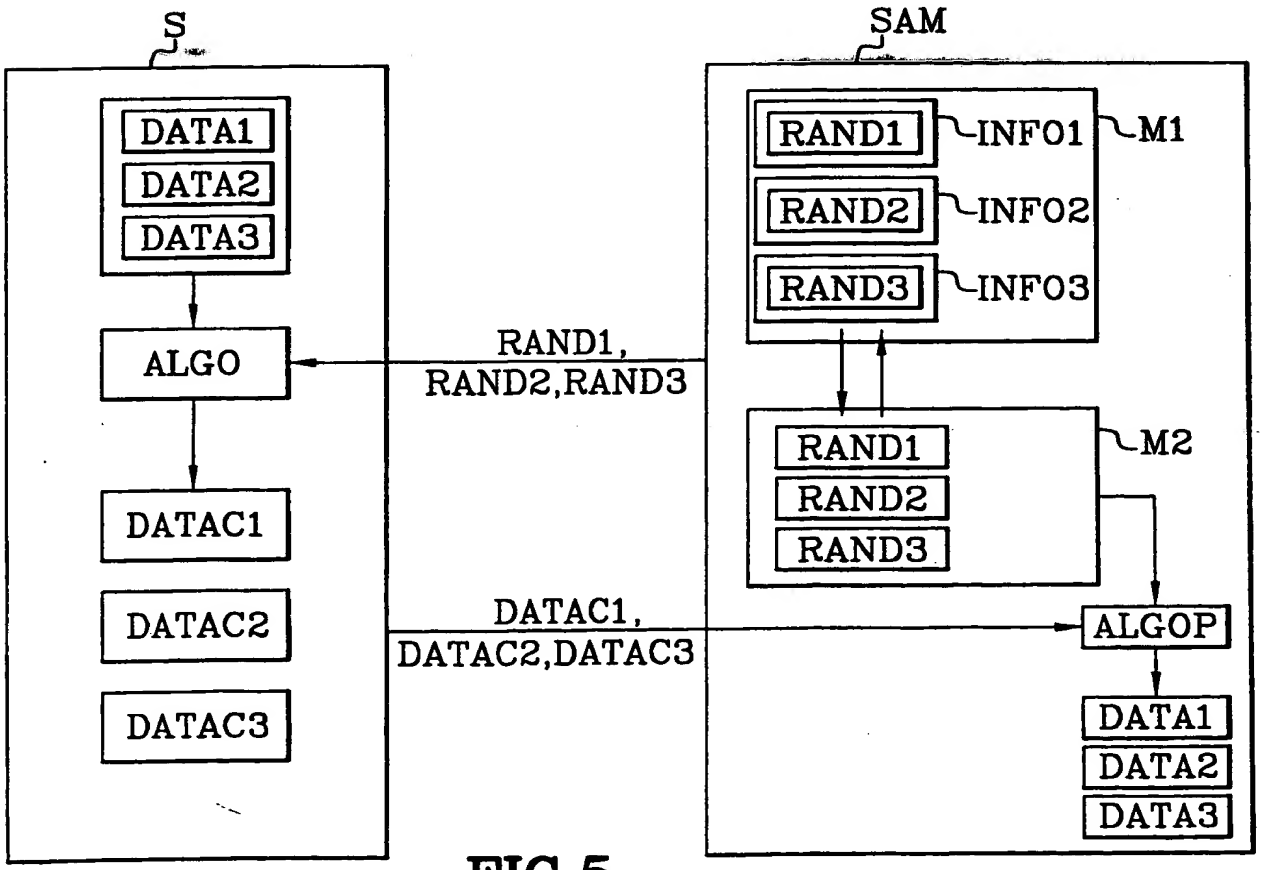
S
SAM
DATA1
DATA2
DATA3
ALGO
DATAC1
DATAC2
DATAC3
RAND1
INFO1
M1
RAND2
INFO2
RAND3
INFO3
RAND1,
RAND2,RAND3
RAND1
RAND2
RAND3
M2
DATAC1,
DATAC2,DATAC3
ALGOP
DATA1
DATA2
DATA3

FIG.5